REMARKS

In response to the Office Action dated 25 September 2001, claims 1-8 have been amended. No new matter has been added. Reexamination and reconsideration of the claims as requested is respectfully requested.

In paragraph 1 on page 2 of the Office Action, claims 1-8 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Lerner et al. in view of Gurnet et al. and further in view of Iwamura et al.

According to the Office Action, Lerner discloses an encryption key management system and method of securely communicating data. However, according to the Office Action, Lerner does not disclose calculating encryption and decryption keys, generating authenticated code, numbering the messages with sequence numbers, transmitting the sequence number with the message, and using the latest sequence number as input for recalculation of the security parameters that includes cryptographic key and authenticated code.

Nevertheless, according to the Office Action, Gurney discloses a keyless entry system that comprises steps of: numbering messages with sequence numbers, transmitting the sequence number with the message, generating authenticated MAC code based on the latest sequence number. Further, according to the Office Action, Iwamura discloses a method and network for communicating between a group of entities a text encrypted that comprises the step of calculating encryption and decryption keys by a random number.

Therefore, according to the Office Action, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the system as

B

Applicant respectfully disagrees with the Office Action's assertion that Lerner teaches monitoring of the interval for updating encryption and decryption keys. Lerner does not teach a changeable interval.

Gurney fails to remedy the deficiencies of Lerner. Gurney fails to disclose at least reaching agreement between communicating parties on an interval for recalculation of the security parameters. Rather, Gurney discloses a system for numbering messages with sequence numbers, transmitting the sequence number with the message, and generating authenticated code based on the latest sequence number. In Gurney, a new authentication code is generated for each message.

Iwamura fails to remedy the deficiencies of Lerner and Gurney. Iwamura fails to disclose at least reaching agreement between communicating parties on an interval for recalculation of the security parameters. Rather, Iwamura describes how two parties can agree on use of an encryption/decryption keys by the help of a third party.

In contrast, Applicant's invention discloses that parties may agree on the security parameter recalculation. This aspect of the Applicant's invention is supported by the Specification in a variety of places, for example, Applicant's invention describes the security parameter recalculation, in which "[t]he recalculation can be based on a shared secret and the latest sequence number, for example. Security parameters can also be used to calculate session keys Kn for ciphering and the message authentication code MAC in the following way, for example:

Kn = H(S, N)

MAC = H(M, S, N),

B

Appendix A
Marked Up Version of the Entire Claim Set

Please amend claims 1-8 as follows.

1. (Amended) [Method] A method for providing connection security for the transmission between communicating parties in a telecommunication network, the method comprising the steps of:

exchanging security parameters between communicating parties,

providing connection security for messages based on these security parameters, [and]

transmitting said messages between communicating parties,

[characterized in that] wherein the method further comprises the steps of:

reaching agreement between communicating parties on an interval for recalculation of the security parameters,

monitoring of the interval for recalculation by the communicating parties,

recalculating the security parameters at the agreed interval, and

providing connection security for messages based on the latest recalculated security parameters.

2. (Amended) [Method] The method according to claim 1, [characterized in that] wherein providing connection security for messages based on the latest recalculated security parameters comprises the step of

ciphering messages based on the latest recalculated security parameters.

B

3. (Amended) [Method] The method according to claim 1, [characterized in that] wherein providing connection security for messages based on the latest recalculated security parameters comprises the step of

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

4. (Amended) [Method] The method according to claim 1, [characterized in that] wherein providing connection security for messages based on the latest recalculated security parameters comprises the steps of

ciphering messages based on the latest recalculated security parameters, and

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

5. (Amended Twice) [Method] The method according to claim 3, [characterized in that] wherein authenticating and providing integrity for the messages is arranged with a message authentication code MAC.

6. (Amended) [Method] The method according to claim 1, [characterized in that] wherein the method further comprises the steps of:

numbering the messages,

agreeing on the number of messages to determine the interval for the recalculation of the security parameters,

recalculating the security parameters after the agreed number of messages have been transmitted.

B

7. (Amended) [Method] The method according to claim 6, [characterized in that] wherein the method further comprises the steps of:

numbering the messages with sequence numbers,

transmitting the sequence number with the message, and

using the latest sequence number as input for recalculation of the security parameters.

8. (Amended) [Method] The method according to claim 1, [characterized in that] wherein the method comprises the step of

reaching agreement between communicating parties during handshaking on the interval for recalculation of the security parameters.

B